



## 【特許請求の範囲】

【請求項1】 電子請求書処理システムであって、

複数の顧客のための複数の完全な請求書をストアするデータベースを有するビラーコンピュータと、

前記ビラーコンピュータに結合され、各完全な請求書の概要および前記ビラーコンピュータによってデジタル方式で署名された各完全な請求書のそれぞれのハッシュをストアするデータベースを有する、請求書提示コンピュータと、

前記ビラーコンピュータおよび前記請求書提示コンピュータに結合された多数の顧客コンピュータとを含み、特定の顧客コンピュータ各々は、a) 選択された完全な請求書の概要とそのそれぞれのデジタル方式で署名されたハッシュとを要求し前記請求書提示コンピュータから受取り、かつb) 前記選択された完全な請求書を要求し前記ビラーコンピュータから受取る、電子請求書処理システム。

【請求項2】 前記特定の顧客コンピュータは、a) 前記選択された完全な請求書の新しいハッシュを発生させ、b) 前記選択された完全な請求書の前記デジタル方式で署名されたハッシュを解読し、かつc) もし解読されたデジタル方式で署名されたハッシュが前記新しく発生されたハッシュと等しくなければ、不一致が存在することを示すことによって、前記選択された完全な請求書の受取に応答する、請求項1に記載の電子請求書処理システム。

【請求項3】 前記特定の顧客コンピュータはまた、前記請求書提示コンピュータに支払メッセージを送り、該支払メッセージは、a) 前記選択された完全な請求書の前記デジタル方式で署名されたハッシュ、およびb) 前記選択された完全な請求書に対する指定された額の資金の支払許可を含み、両者は前記特定の顧客コンピュータによってデジタル方式で署名されている、請求項1に記載の電子請求書処理システム。

【請求項4】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって、1つのまとまった統一体として署名される、請求項3に記載の電子請求書処理システム。

【請求項5】 前記支払メッセージにおいて、前記選択された完全な請求書

の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は各々、前記特定の顧客コンピュータによって別個に署名される、請求項3に記載の電子請求書処理システム。

【請求項6】 前記請求書提示コンピュータは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対しての指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによってデジタル方式で署名されているが、前記支払メッセージから獲得されたままで、前記請求書提示コンピュータのデータベースにストアすることによって、前記支払メッセージに応答する、請求項3に記載の電子請求書処理システム。

【請求項7】 前記ビラーコンピュータおよび前記顧客コンピュータと相関づけられるそれぞれの口座を保持する電子支払サブシステムをさらに含み、前記請求書提示コンピュータは、前記指定された額の資金の、前記特定の顧客コンピュータ用の口座から前記ビラー口座用の口座への移転の要求を、前記支払サブシステムへ送ることによって、前記支払メッセージに応答する、請求項3に記載の電子請求書処理システム。

【請求項8】 前記支払サブシステムは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対する指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによりデジタル方式で署名されているが、前記支払メッセージから獲得されたままで含む、決算記録をストアする、請求項7に記載の電子請求書処理システム。

【請求項9】 前記請求書提示コンピュータはまた、a) 要求された移転が行なわれたかまたは拒否されたかを示す応答を前記支払サブシステムから受取り、かつb) 前記応答を反映するようそのデータベースを更新する、請求項7に記載の電子請求書処理システム。

【請求項10】 前記請求書提示コンピュータはまた、請求書の支払が許可されたか否か、および前記支払サブシステムにおいて指定された額の資金が移転されたかまたは拒否されたかを示すメッセージを発生し前記ビラーコンピュータ

に送る、請求項9に記載の電子請求書処理システム。

【請求項11】 前記請求書提示コンピュータはまた、前記支払サブシステムにおいて、許可された資金の移転が行なわれたかまたは拒否されたかを示すメッセージを発生し各顧客コンピュータに送る、請求項9に記載の電子請求書処理システム。

【請求項12】 前記ビラーコンピュータおよび前記顧客コンピュータに相関付けされるそれぞれの口座を保持する電子支払サブシステムをさらに含み、前記特定の顧客コンピュータはまた、前記支払サブシステムに支払メッセージを送り、該支払メッセージは、a) 前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよびb) 前記選択された完全な請求書に対しての指定された額の資金の支払の許可を含み、両者は前記特定の顧客コンピュータによりデジタル方式で署名される、請求項1に記載の電子請求書処理システム。

【請求項13】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって、1つのまとまった統一体として署名される、請求項12に記載の電子請求書処理システム。

【請求項14】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は各々、前記特定の顧客コンピュータによって別個に署名される、請求項12に記載の電子請求書処理システム。

【請求項15】 前記支払サブシステムは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対する指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによりデジタル方式で署名されているが、前記支払メッセージにおいて獲得されたままで含む、決算記録をストアする、請求項12に記載の電子請求書処理システム。

【請求項16】 電子請求書処理システムであって、

複数の顧客に対し完全な請求書を発生し、ビラーコンピュータによってデジタル方式で署名された各完全な請求書のそれぞれのハッシュを発生させるビラーコ

ンピュータと、

前記ビラーコンピュータに結合された多数の顧客コンピュータとを含み、各特定の顧客コンピュータは支払メッセージを発生し、該支払メッセージは、a) 前記ビラーコンピュータによってデジタル方式で署名された選択された完全な請求書のハッシュおよびb) 前記選択された完全な請求書に対しての指定された額の資金の支払の許可を含み、アイテムa) およびb) は両方とも前記特定の顧客コンピュータによって前記支払メッセージにおいてデジタル方式で署名され、前記システムはさらに、

前記顧客コンピュータに結合された支払サブシステムを含み、該支払サブシステムは前記支払メッセージからの、前記特定の顧客コンピュータによりデジタル方式で署名されたアイテムa) およびb) を含む決算記録をストアする、電子請求書処理システム。

【請求項17】 争い解決手段をさらに含み、該争い解決手段は、前記ビラーコンピュータおよび前記特定の顧客コンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュを前記決算記録から読取り；前記デジタル方式で署名されたハッシュを解読して、署名されていない形の前記ハッシュを獲得し；争われている完全な請求書の新しいハッシュを発生し；前記新しいハッシュを署名されていない形の解読されたハッシュと比較する、請求項16に記載の電子請求書処理システム。

【請求項18】 争い解決手段をさらに含み、該争い解決手段は、前記特定の顧客コンピュータによってデジタル方式で署名された指定された額の資金の支払の前記許可を前記決算記録から読取り；前記デジタル方式で署名された許可を解読して、署名されていない形の前記指定された資金の額を獲得し；前記署名されていない指定された資金の額と支払ったとして争われている支払の額とを比較する、請求項16に記載の電子請求書処理システム。

【請求項19】 前記支払メッセージにおいて、前記ビラーコンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって1つのまとまった統一体として署名される、請求項16に記載の電子請

求書処理システム。

【請求項20】 前記支払メッセージにおいて、前記ビラーコンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって各々別個に署名される、請求項16に記載の電子請求書処理システム。

【請求項21】 前記ビラーコンピュータおよび前記多数の顧客コンピュータに結合され、各完全な請求書の概要をストアし、前記ビラーコンピュータによりデジタル方式で署名された各完全な請求書の前記それぞれのハッシュをストアする請求書提示コンピュータをさらに含み、各顧客コンピュータは、a) 選択された完全な請求書の概要とそのそれぞれのデジタル方式で署名されたハッシュとを要求し、前記請求書提示コンピュータから受取り、b) 前記選択された完全な請求書を要求し、前記ビラーコンピュータから受取る、請求項16に記載の電子請求書処理システム。

## 【発明の詳細な説明】

## 【0001】

## 【発明の背景】

この発明は、それによって請求書が提示され支払われる電子システムに関する。

## 【0002】

先行技術による請求書提示および支払システムの1つが、米国特許第5,465,206号（以下Visa特許と呼ぶ）の図1に開示されている。このシステムでは、顧客は、ビラー（請求書発行者）から請求書を受取り、これに応答して顧客はビラーに小切手を郵便で送り返す。ビラーは、支払を受けるためこの小切手をビラーの銀行に提示する。ビラーの銀行は、小切手を決済銀行へ送り、決済銀行はビラーの銀行と顧客の銀行との間での資金の移転を清算し決済する。この決済ステップに続いて、ビラーの銀行によって資金は引出し可能なビラーの口座へと移転される。

## 【0003】

（Visa特許の図2Aおよび図2Bに開示される）先行技術による第2の請求書提示および支払システムにおいては、顧客は、ビラーからの請求書に対してサービス局に電子的にメッセージを送ることで応答し、この電子メッセージがサービス局に対して請求書の支払を許可する。メッセージを受取ると、サービス局は、顧客の銀行の顧客の口座の小切手を書き、この小切手を支払のためにサービス局の銀行に提示する。するとサービス局の銀行は、小切手を決済銀行へ送り、決済銀行がサービス局の銀行と顧客の銀行との間での資金の移転を清算し決済する。このステップシーケンスが、ビラーの多くの顧客について多数繰返される。その後、サービス局はビラーに、支払済みの請求書すべてのリストを支払済み総額に対する1つの小切手とともに送る。

## 【0004】

（Visa特許の図3に開示される）先行技術による第3の請求書提示および支払システムにおいては、ビラーは、顧客の銀行の顧客の口座から規則的な定期的支払を受け、こうした支払は顧客によってではなくビラーによって開始される。こ

の方法では、ビラーは、顧客、定期的支払額、および各支払の期限日を特定するファイルを維持する。各支払の開始のため、ビラーはビラーの銀行に支払要求を電子的に送り；そしてこれに应答して、ビラーの銀行は自動手形交換所（ACH）によって要求される所定の標準フォーマットで借方要求を出す。この借方要求は、ビラーの銀行が他の顧客に対して出したすべての他のACH借方要求および信用貸し要求とともに、ビラーの銀行にストアされる。その後、ACH借方要求および信用貸し要求のバッチは、連邦準備局または他のACH手形交換機関に電子的に送信され；この送信によって、ビラーの銀行と機構の銀行との間の純勘定が決済される。

【 0 0 0 5 】

（Visa特許の図4から図12に開示される）先行技術の第4の請求書提示および支払システムにおいては、ビラーの銀行、顧客の銀行および決済銀行がすべて電子支払ネットワークによって相互結合されている。この方法では、ビラーからの請求書に対し、顧客は顧客の銀行に請求書に対する支払をするよう命令することで应答する。これに应答して、顧客の銀行は、請求書の支払のため十分な資金が利用可能であるか否か、または資金が利用可能でないならば顧客の銀行が損失の危険を犯す意思があるか否かを判定するため、顧客の口座を調べる。いずれかの判定がなされれば、顧客の銀行は、支払ネットワークを通じてビラーの銀行へ支払メッセージを電子的に送る。このような支払メッセージ各々は、また、支払ネットワーク内にストアされ、顧客の銀行とビラーの銀行との間ですべての支払メッセージによって移転されている資金の網を作る決済サブシステムによって取り扱われる。その後、決済サブシステムは、決済銀行に対して移転命令を電子的に送り、決済銀行は顧客の銀行とビラーの銀行との間での純勘定を決済する。この決済ステップによって、ビラーの銀行によりビラーの口座へ資金が移転される。

【 0 0 0 6 】

しかし、これらの先行技術によるシステムすべてにおける主な欠点は、請求書に対する支払が行なわれる前に顧客に対し請求書を電子的に提示するための手段が設けられていないことである。図1、図2および図4のシステムにおいては、



請求書は従来の郵便局による配達によって顧客に物理的に届けられ；図3のシステムにおいては、請求書は顧客に全く送られることなく支払が行なわれる。

【0007】

さらに、もし上述の先行技術によるシステムが、請求書が郵便ではなく電子的に送られるように何らかの形で変更されたならば、新しい問題が発生し得る、なぜならば顧客は請求書の額を確定する何の文書もビラーから得られないだろうからである。その結果、顧客による支払が行なわれた後に、ビラーが請求書において要求されている額を増やし、その増やされた額が元の請求書にも入っていたと主張することがあり得る。

【0008】

また、もし上述の先行技術によるシステムが、小切手がなくされすべての支払が電子的に行なわれるように何らかの形で変更されたならば、他の新しい問題が生じ得る、すなわち、支払を許可された額を確定するための用済み小切手が発生しない。この結果、一定額の資金の支払が電子的に行なわれた後に、顧客がこれよりも少額の支払しか許可していないと後から主張することがあり得、および／または、ビラーがより高額の支払が許可されていたと後から主張したりし得る。

【0009】

したがって、この発明の主な目的は、ビラーおよび／または顧客による詐欺を防止するためハッシュおよびデジタル署名を用いる完全電子請求書提示および支払システムを提供することである。

【0010】

【発明の概要】

この発明の好ましい一実施例を構成する、完全電子請求書提示および支払システムは、複数の顧客に対する複数の完全な請求書をストアするデータベースを有するビラーコンピュータと、ビラーコンピュータに結合され、各完全な請求書の概要およびビラーコンピュータによってデジタル方式で署名された各完全な請求書の各々のハッシュをストアするデータベースを有する請求書提示コンピュータを含む。また、この実施例は、ビラーコンピュータおよび請求書提示コンピュータに結合された多数の顧客コンピュータを含み、各特定の顧客コンピュータは

、 a ) 選択された完全な請求書の概要およびそのそれぞれのデジタル方式で署名されたハッシュを要求し請求書提示コンピュータから受取ることができ、かつ b ) 選択された完全な請求書を要求しビラーコンピュータから受取ることができる。

【 0 0 1 1 】

ビラーコンピュータ内の選択された完全な請求書の概要が請求書提示コンピュータ内にストアされた後に、ビラーコンピュータ内の選択された完全な請求書が変更されていないことを確実にするため、特定の顧客コンピュータはビラーコンピュータから受取られたままの選択された完全な請求書の新しいハッシュを発生し、請求書提示コンピュータから受取られたままの選択された完全な請求書のデジタル方式で署名されたハッシュを解読する。もし、新しいハッシュが解読されたハッシュと等しくなければ、顧客コンピュータは、不一致が存在するため請求書に対する支払がされるべきではないことを示すメッセージを表示する。

【 0 0 1 2 】

もし新しいハッシュと解読されたハッシュとが等しければ、特定の顧客コンピュータから請求書提示コンピュータへ支払メッセージを送ることができ；この支払メッセージは、 a ) 選択された完全な請求書のデジタル方式で署名されたハッシュおよび b ) 選択された完全な請求書に対する指定された額の資金の支払の許可を含み、両者は特定の顧客コンピュータによりデジタル方式で署名される。好ましくは、この支払メッセージは、請求書提示コンピュータのデータベース内および請求書提示コンピュータに結合する電子支払サブシステムの決算記録内にストアされる。

【 0 0 1 3 】

その後、ストアされた支払メッセージは、ビラーと顧客との間で生じ得る一定の争いを解決するために使用できる。もし争いの論点が、支払が許可された後に請求書が変えられたか否かというものであれば、ビラーコンピュータおよび特定の顧客コンピュータによりデジタル方式で署名された選択された完全な請求書のハッシュを決算記録から読取り；デジタル方式で署名されたハッシュを解読して署名されていない形のハッシュを獲得し；現在ビラーコンピュータ内にストアさ

れているままの完全な請求書の新しいハッシュを発生し；そして新しいハッシュと署名されていない形の解読されたハッシュとを比較する、争い解決手段によって解決される。比較誤り (miscompare) は、支払が許可された後に完全な請求書が変更されたことを示す。

【 0 0 1 4 】

もし争いの論点が、選択された請求書に対し行なわれたと主張されている支払が行なわれたか否かというものであれば、特定の顧客コンピュータによってデジタル方式で署名された指定された額の資金の支払の許可を決算記録から読取り；デジタル方式で署名された許可を解読して署名されていない形の指定された額の資金を獲得し；そして署名されていない指定された資金額とを支払が行なわれたと主張されている支払額とを比較する、争い解決手段によって解決される。もし比較誤りが生じれば、行なわれたと主張されている支払は許可されておらず、したがって支払が行なわれていないことになる。

【 0 0 1 5 】

デジタル方式で署名されたハッシュ各々は、16から32バイトからなることが好ましく、一方各完全な請求書は数千バイトからなることが典型的である。したがって完全な請求書全体ではなく完全な請求書のハッシュをストアすることによって、請求書提示コンピュータのデータベース内および支払サブシステムの決算記録内の総記憶量が大きく減じられる。

【 0 0 1 6 】

【 詳細な説明 】

図1に、この発明の好ましい一実施例を構成する電子請求書処理システムが示される。図1実施例は、多数のビラーコンピュータ10-n（ただしnは1、2、…Nに等しい）、単一の請求書提示コンピュータ20および多数の顧客コンピュータ30-m（ただしmは1、2、…Mに等しい）を含む。これらのコンピュータ10-n、20および30-mはすべて、通信チャネル41、42および43によって図示されるように相互結合される。

【 0 0 1 7 】

各ビラーコンピュータ10-nは、さまざまな顧客についての詳細な販売およ

びサービスデータ12をそこで受取る入力11を有し；このデータ12はビラーコンピュータ10-n内のデータベース13内にストアされる。ここで、データ12は各顧客に対する1または2以上の完全な請求書として整理される。図1において、特定の完全な請求書の1つがCBILLで示され、典型的なCBILLの1つの例が図2Aおよび図2Bに示される。

【0018】

図2Aおよび図2BのCBILLを調べると、CBILLが、請求金のかかった個別のアイテムのいくつかのリスト14a~14eを含むことが示される。図2Aおよび図2Bでは場所の節約のため、個別に請求金のかかったアイテムの多くは、一連の3つの点で置換えられ；しかし、実際のCBILLにおいては、個別に請求金のかかったアイテムすべてが示される。また、図2Aおよび図2BのCBILLは、広告15a、会社のロゴ15bおよび15c、一定期日までに支払われるべき総額が支払われなかった場合に課される罰金の残額15dなど不必要な情報を含む。

【0019】

各ビラーコンピュータ10-nはまた、以下のように、そのデータベース13内で各CBILLに対して動作するプログラム16を含む。第1に、プログラム16は完全な請求書の概要を発生し、この概要は図1ではSBILLで示される。図3は、図2Aおよび図2BのCBILLに対するSBILLの一例を示す。不必要な情報15a~15dを取除き、リスト14a~14eを1つの支払われるべき総額で置換えることによって、図3のSBILLは、図2Aおよび図2BのCBILLよりも少なくとも20分の1の短さとなる。

【0020】

請求書の概要が発生された後、プログラム16は、完全な請求書のハッシュを発生し；そして次にプログラム16は、ビラーコンピュータ・プライベートキーを使用してハッシュにデジタル方式で署名する。署名前のこのハッシュは、図1でH(CBILL)で示され；デジタル方式で署名されたハッシュは図1でS。

(H(CBILL))で示され；S。は、署名がビラーコンピュータ内のプライベートキー「b」で行なわれたことを示す。次に、プログラム16は請求書の概

要S B I L Lとデジタル方式で署名されたハッシュS。(H (C B I L L)) を含む請求書提示コンピュータ20へ、ポスティング要求を送る。

【0021】

請求書提示コンピュータ20内には、請求書概要S B I L Lおよびデジタル方式で署名されたハッシュS。(H (C B I L L)) を受取るプログラム21が含まれる。このプログラム21は、請求書概要S B I L Lおよびデジタル方式で署名されたハッシュS。(H (C B I L L)) を、請求書提示コンピュータ内のデータベース22内にストアすることによって、これらをポスティングする。プログラム21はまた、請求書概要S B I L Lおよびデジタル方式で署名されたハッシュS。(H (C B I L L)) が現在ポスティングされていることを示す請求書状態コード「1」をデータベース22にストアする。→初期状態(未決済)

【0022】

各顧客コンピュータ30-mは、請求書提示コンピュータ20およびビラーコンピュータ10-nと相互作用するプログラム31を含み、プログラム31の詳細は図4に示される。まず、プログラム31は顧客コンピュータ30-mのオペレータから現在の未払請求書リスト(L C U B)を表示するよう要求を受取る。顧客コンピュータは、応答して、請求書提示コンピュータ20へ要求が送られる図4のステップS1を実行する。この要求は、請求書提示コンピュータにおいてプログラム23により受取られ、プログラム23はデータベース22を調べ要求されたリストを発生させる。次に、要求された現在の未払請求書リストは、顧客コンピュータ30-mへ送られ、顧客コンピュータにおいて図4のステップS2で示されるように、リストは受取られプログラム31により表示される。

【0023】

その後、顧客コンピュータ30-mのオペレータは、リスト中の特定の請求書概要S B I L Lを見たいという要求を出すことができる。プログラム31は応答して、図4のステップS3に示されるようにこの特定の請求書概要についての要求を請求書提示コンピュータへ送る。次に、請求書提示コンピュータ20内のプログラム23は、要求された請求書概要と、対応する完全な請求書のデジタル方式で署名されたハッシュとをデータベース22から獲得する。概要と署名された

ハッシュとは次に、顧客コンピュータへ送られ、顧客コンピュータにおいて図 4 のステップ S 4 のように受取られる。また、請求書提示コンピュータは、それが送った請求書概要の状態コードを「2」へ変え、それによって、その請求書が顧客コンピュータによって検査されたことを示す。

【 0 0 2 4 】

次に、図 4 のステップ S 5 において、顧客コンピュータ 30-m 内のプログラム 31 が受取った請求書概要を表示する。次に請求書概要に示されるものに基づいて、顧客コンピュータ 30-m のオペレータはどのように処理を進めるかについていくつかの選択肢 S 6 a ~ S 6 d を有する。選択肢 S 6 a の場合、表示中の請求書概要に対応する完全な請求書を表示するよう要求が出される。選択肢 S 6 b では、支払サブスクリーンに対する要求が行なわれ、それによって、概要が表示中の請求書に対し選択可能な額の資金を支払うことができる。選択肢 S 6 c では、ステップ S 1 に戻ることができ、それによって、現在の未払請求書リストが再び表示されるであろう。選択肢 S 6 d では、請求書提示コンピュータ 20 とビラーコンピュータ 10-m との相互作用を終了することができる。これらの選択肢は、図 3 の請求書概要の下に示されており；マウスによってカーソルを所望の選択肢の上に動かし「クリックする」ことによって特定の選択肢が選択される。

【 0 0 2 5 】

選択肢 S 6 a が選択されると、顧客コンピュータ 30-m は、ステップ S 11 ~ S 15 を含むプログラム 31 内のサブルーチン 31 a を実行する。ステップ S 11 で、顧客コンピュータ 30-m は、表示中の請求書概要に対応する特定の完全な請求書に対する要求をビラーコンピュータ 10-n へ送る。各ビラーコンピュータはプログラム 17 を含み、プログラム 17 は、要求された完全な請求書であるはずの完全な請求書をそのデータベース 13 から引出し、引出された完全な請求書を顧客コンピュータ 30-m へ送ることで、このような要求に応答する。この完全な請求書は、図 2 A および図 2 B 内でサブルーチン 31 a によりステップ S 12 のように、顧客コンピュータにおいて受取られる。

【 0 0 2 6 】

次にステップ S 13 において、サブルーチン 31 a は、ビラーのコンピュータ

に対しパブリックキーを使用してデジタル方式で署名されたハッシュS。(H (C B I L L)) を解読する。このステップにより、完全な請求書のハッシュが暗号化されていない形、H (C B I L L) として獲得される。次にステップS 1 4において、サブルーチン3 1 aは、ステップS 1 2においてビラーのコンピュータ1 0 - nから獲得した完全な請求書についての新しいハッシュを再び計算する。そしてステップS 1 5において、サブルーチン3 1 aは、ステップS 1 3で解読されたハッシュとステップS 1 4で新しく再び計算されたハッシュとを比較する。

#### 【 0 0 2 7 】

もし比較された2つのハッシュが等しくなければ、オペレータに不一致の警告を出すメッセージが表示される。不一致に対する考えられる原因の1つは、ビラーのコンピュータ1 0 - n内の完全な請求書が、完全な請求書の概要C B I L Lおよびそのデジタル方式で署名されたハッシュが請求書提示コンピュータ2 0内にポスティングされた後に変更されたというものである。したがって、不一致メッセージを表示することで、顧客は、ビラーコンピュータから引出されたままの現在の完全な請求書が請求書提示コンピュータ内にポスティングされたままのその概要と一致しない場合に請求書に対し支払を行なうことから保護される。

#### 【 0 0 2 8 】

逆に、ステップS 1 5において比較された2つのハッシュが等しければ、顧客コンピュータ3 0 - m上に要求された完全な請求書が表示される。これは図4のステップS 2 0のように行なわれる。次に表示された完全な請求書が示すものに基づいて、顧客コンピュータ3 0 - mのオペレータは、どのように処理を進めるかについていくつかの選択肢S 2 1 a ~ S 2 1 cを有する。

#### 【 0 0 2 9 】

選択肢S 2 1 aでは、支払サブスクリーンに対する要求が行なわれ、それによって表示中の完全な請求書に対し選択可能な額の資金を支払うことができる。選択肢S 2 1 bでは、最初のステップS 1に戻ることができ、そこで、現在の未払請求書リストが再び表示されるであろう。選択肢S 2 1 cでは、請求書提示コンピュータ2 0とビラーコンピュータ1 0 - mとの相互作用を終了することができ

る。

【0030】

選択肢S21aが選択された場合、顧客コンピュータ30-mはステップS22を実行し、それによって顧客コンピュータ30-mのオペレータは請求書に対して支払われるべき額Xドルを入力する。次に選択肢S23によって、オペレータはこのような支払行為を許可できる。許可に応答して、顧客コンピュータは、支払要求メッセージ(PRM)が、請求書提示コンピュータ20へ送られるステップS24を実行する。この支払要求メッセージは、a)ビラーコンピュータによりデジタル方式で署名された選択された完全な請求書のハッシュ、およびb)選択された完全な請求書に対しての指定された額Xドルの資金の支払の許可を含む。また、プログラム31は、これらのアイテムa)およびb)の両方にデジタル方式で署名をするため、顧客コンピュータのプライベートキーを使用し、これは、図4のステップS24にS.[\$X, S.(H(CBILL)) ]として示される。ここで、S.は顧客コンピュータ内のプライベートキー「C」で行なわれた署名を示す。

【0031】

ステップS24において支払額Xドルが顧客コンピュータによりS.として署名されるという事実のため、ビラーは、顧客によって顧客がより高い金額を払ったと後から主張されることから保護される。また、ステップS24において完全な請求書のハッシュが顧客コンピュータによって署名されているという事実により、ビラーは、顧客の請求書の額が変えられていると顧客によって後から主張されることから保護される。

【0032】

ここで、図4において、顧客コンピュータのオペレータが、選択肢S6bを選択し、完全な請求書を見ることなく請求書概要上の支払サブスクリーンに対する要求がなされたと考える。選択肢S6bが選択されるとき、図4のプログラムは自動的に上述のサブルーチン31aを実行する。そして支払が許可されれば、図4のプログラムはステップS24を実行する。サブルーチン31aを実行することで、顧客は再び、完全な請求書とその概要とが一致していない請求書について



の支払を行なうことから保護される。ステップS 2 4を実行することで、ビラーは再び、支払を顧客が許可した金額について争うおよび／または顧客が受取った請求書において支払われるべき金額について争う顧客に対して保護される。

【 0 0 3 3 】

次に図5を参照し、図5は、電子支払サブシステム50と関連して請求書提示コンピュータ20によってどのように支払要求メッセージPRMが処理されるかを示す。この支払サブシステム50においては、各顧客は、顧客の銀行においてコンピュータX ( i ) により維持される口座を有し、各ビラーは、ビラーの銀行にコンピュータX ( j ) により維持される口座を有する。コンピュータX ( i ) およびX ( j ) はすべて、互いにそして清算および決済銀行にある他のコンピュータYへ結合される。

【 0 0 3 4 】

支払要求メッセージPRMが顧客コンピュータ30-mから送られるとき、メッセージは請求書提示コンピュータ20内のプログラム24により受取られる。これは図5の時刻t 1で起こる。そして、プログラム24は、受取られた支払要求メッセージに応答して、データベース22へアクセスし、支払われるべき請求書の状態を、支払が要求されたことを示すコード「3」に変える。これは図5の時刻t 2で起こる。

【 0 0 3 5 】

次に、請求書提示コンピュータ20内のプログラム24は、支払を許可した顧客の口座を維持する銀行のコンピュータX ( i ) に支払要求メッセージを送る。そこで、支払要求メッセージはプログラム51 aにより受取られる。これは図5の時刻t 3で起こる。プログラム51 aは、これに応答して、支払を許可した顧客の口座が入っている顧客コンピュータX ( i ) 内のデータベース51 bにアクセスする。このステップにより、プログラム51 aは、許可された支払をカバーするのに十分なだけの額の資金が顧客の口座に入っていることを確かめる。このステップは図5の時刻t 4で起こる。

【 0 0 3 6 】

もし十分な資金が見つければ、コンピュータX ( i ) は、支払を受取るべきビ

ラーの銀行内のコンピュータ X ( j ) にメッセージを送る。図 5 の時刻 t 5 で生じるこのメッセージは、ビラーの口座の確認を要求する。コンピュータ X ( j ) 内のプログラム 5 2 a は、応答して、支払を受けるべき特定ビラーの口座を含むデータベース 5 2 b にアクセスする。これは図 5 の時刻 t 6 で起こる。そして、コンピュータ X ( j ) 内のプログラム 5 2 a は、ビラーの口座が見つかったか、そしてそれが適切なものであるか否かを示すリターンメッセージをコンピュータ X ( j ) 内のプログラム 5 1 a に送り返す。

【 0 0 3 7 】

もしビラーの口座が適切であれば、コンピュータ X ( i ) は支払要求メッセージにおいて許可された資金の移転を実際に行なうよう要求するメッセージを清算および決済コンピュータ Y へ送る。図 5 の時刻 t 7 において送られるこの要求は、コンピュータ Y 内のプログラム 5 3 a により受取られる。プログラム 5 3 a は応答して、コンピュータ X ( i ) および X ( j ) を備える銀行についての純勘定を保持するデータベース 5 3 b にアクセスする。もしこれらの口座が適切なものであれば、プログラム 5 3 a は、コンピュータ X ( i ) を備える銀行に対しての純勘定から支払われるべき金額を引き、コンピュータ X ( j ) を備える銀行についての純勘定に支払われる金額を加算する。これは図 5 の時刻 t 8 で起こる。

【 0 0 3 8 】

上述のように純勘定が変更された後、時刻 t 9 において、プログラム 5 3 a は、支払要求メッセージについての決算記録がストアされるデータベース 5 3 c にアクセスする。この決算記録は、a) ビラーコンピュータ 1 0 - n によりデジタル方式で署名された選択された完全な請求書のハッシュおよび b) 選択された完全な請求書に対しての指定された額 X ドルの資金の支払の許可を含み、両者は顧客コンピュータ 3 0 - m によりデジタル方式で署名される。これは図 5 に参照番号 5 3 d で示される。

【 0 0 3 9 】

この後、コンピュータ Y は、決済が成功したか否かを示すメッセージをコンピュータ X ( i ) および X ( j ) へ送る。これは図 5 の時刻 t 1 0 で行なわれる。もし決済が行なわれれば、コンピュータ X ( j ) 内のプログラム 5 2 a は、許可

された支払額だけビラーの口座の額を増加させ、コンピュータ X ( i ) 内のプログラム 5 1 a は許可された支払額だけ顧客の口座の額を減少させる。

【 0 0 4 0 】

この後、コンピュータ X ( i ) は、支払要求メッセージにおいて許可されたように支払が決済されたか否かを示すメッセージを請求書提示コンピュータ 2 0 へ送る。請求書提示コンピュータ 2 0 内のプログラム 2 4 は応答して、支払が要求された請求書についての状態コードをコード「4」または「5」に変える。コード「4」は決済が行なわれたことを示し、コード「5」は決済が拒否されたことを示す。

【 0 0 4 1 】

上に説明した電子請求書処理システムの主な特徴の1つは、清算および決済コンピュータ Y の支払決算記録 5 3 c 内のアイテム 5 3 d が、顧客とビラーとの間で生じ得る争いを解決するための手段を提供することである。図 6 中、どのようにしてこのような争いが解決されるのかを示すプロセスが示される。図 6 のステップはすべてコンピュータ Z によって行なわれるが、コンピュータ Z は、清算および決済コンピュータ Y の支払決算記録 5 3 c の争われている請求書についてアイテム 5 3 d にアクセスする許可およびビラーコンピュータ 1 0 - n の争われている請求書へのアクセスの許可を有するコンピュータである。

【 0 0 4 2 】

まず、図 6 のステップ S 3 1 において、コンピュータ Z は、支払決算記録 5 3 c のアイテム 5 3 d を要求するメッセージを清算および決済コンピュータ Y に送る。コンピュータ Z は、ステップ S 3 2 において応答し、図 6 において S. ( \$ X , S. ( H ( C B I L L ) ) ) として示されるアイテム 5 3 d を受取る。前に説明したように、S. ( H ( C B I L L ) ) はビラーコンピュータ 1 0 - n によりデジタル方式で署名された完全な請求書のハッシュであり、\$ X はこの完全な請求書について支払が許可された資金の額である。S. は、上述のアイテム両方が顧客コンピュータ 3 0 - m によりデジタル方式で署名されていることを示す。

【 0 0 4 3 】

次に、ステップ S 3 3 において、コンピュータ Z は、顧客コンピュータ 3 0 -

mに対してパブリックキーを使用してS.(\$X, S.(HCBILL))を解読する。このステップにより、額\$XおよびS.(H(CBILL))が署名されていない形で獲得される。次にステップS34において、コンピュータZは、額\$Xと、顧客が払ったと主張している額とを比較する。もしこれら2つの額が等しくなければ、コンピュータZが、顧客が支払ったと述べている額を支払っていないことを示す争い解決申告(DRS)用メッセージを発生するステップS35aが実行される。それ以外の場合は、ステップS35bにおいて、コンピュータZは、顧客が払ったと述べている額を実際に払ったことを示すDRSメッセージを発生する。

#### 【0044】

次にコンピュータZはステップS36に進み、S36で、ビラーコンピュータ10-nについてのパブリックキーが獲得される。そしてこのパブリックキーは、S.(H(CBILL))を解読するためコンピュータZによって使用され、それによって、署名されていない形のH(CBILL)が獲得される。次にステップS37において、コンピュータZは、上述の解読されたハッシュを発生するため使用された完全な請求書に対応するはずの現在の完全な請求書を要求するメッセージを、ビラーコンピュータ10-nに送る。この現在の完全な請求書は、ステップS38においてコンピュータZにより受取られ；ステップS39においてコンピュータZは、この現在の完全な請求書を使用して新しいハッシュを再び計算する。

#### 【0045】

そしてコンピュータZは、ステップS40において、ステップS36で獲得されたハッシュH(CBILL)をステップS39で獲得された新しい再び計算されたハッシュと比較する。もしこれら2つのハッシュが等しくなければ、コンピュータZはS41aを実行し、ここで、争われている請求書が金額\$Xがその請求書について支払われた後に変更されていることを示すDRS用メッセージが発生される。それ以外の場合は、ステップS41bが実行され、ここで、コンピュータZは、\$Xの支払が行なわれてから請求書は変更されていないことを示すDRS用メッセージを発生する。

## 【 0 0 4 6 】

最後に、ステップ S 4 2 において、コンピュータ Z は、ステップ S 3 5 a、S 3 5 b、S 4 1 a および S 4 1 b において発生されたメッセージを含むように、D R S を発生する。この D R S は、顧客とビラーとがそれらの争われている請求書についてのその違いを解決するのを助けるため顧客およびビラーに送られる。

## 【 0 0 4 7 】

上に説明した電子請求書処理システムのもう 1 つの主な特徴は、各完全な請求書は単一のコンピュータ、すなわちビラーコンピュータ 1 0 - n にのみストアされるにもかかわらず、いずれの特定の完全な請求書におけるいかなる変化も検出できる点である。この特徴は、ビラーコンピュータによりデジタル方式で署名された各完全な請求書のハッシュを、請求書提示コンピュータ 2 0 および決済コンピュータ Y 内にストアすることにより達成される。このようなデジタル方式で署名されたハッシュは各々、1 6 から 3 2 バイトからなることが好ましく；一方、図 2 A および図 2 B に見られるように、完全な請求書は各々数千バイトからなるのが典型的である。したがって、請求書提示コンピュータ 2 0 のデータベース 2 2 内においておよび清算および決済コンピュータ Y の支払決算記録 5 3 c 内において、総記憶量が著しく減じられる。

## 【 0 0 4 8 】

この発明の好ましい一実施例を構成する電子請求書処理システムを、図 1 から図 6 に関連し詳細に説明した。しかしさらに、この発明の本質および精神から逸脱することなく、この好ましい実施例に一定の変更および修正を加えることができる。

## 【 0 0 4 9 】

たとえば、図 5 において、顧客コンピュータ 3 0 - m は支払要求メッセージ P R M を請求書提示コンピュータ 2 0 へ送り；その後、コンピュータ 2 0 は電子支払サブシステム 5 0 へ支払要求メッセージを送る。これは図 5 の時刻 t 1 および t 3 で行なわれている。しかし、変更例としては、支払要求メッセージは、顧客コンピュータ 3 0 から直接電子支払システム 5 0 へ送ることができ；この変更例は図 7 に示される。

## 【 0 0 5 0 】

図7の電子支払サブシステム50内の構成要素はすべて、図5に示すものと同じであり、それらの動作も、図5に関連して前に説明したのと同じである。したがって、図7の電子支払サブシステム50における参照番号はすべて、図5に示すものと同じである。

## 【 0 0 5 1 】

図7の時刻 $t_1^*$ において、顧客コンピュータ30-mは、支払要求メッセージを電子支払サブシステム50へ直接送る。請求書提示コンピュータ20へは支払要求メッセージは送られない。後に、図7の時刻 $t_{11}^*$ において、顧客コンピュータ30は支払要求メッセージに対する確認または拒否を電子支払サブシステム50から受取る。

## 【 0 0 5 2 】

他の変更例としては、支払要求メッセージは、図5に示したのとは異なる態様で、顧客コンピュータ30-mによってデジタル方式で署名され得る；この変更例も図7に示される。図7の変更例においては、ビラーコンピュータにより署名された選択された完全な請求書のハッシュおよび選択された完全な請求書についての指定された額の資金の支払の許可は、各々、顧客コンピュータ30-mによって別個に署名される。これら2つの別個に署名されたアイテムは、図7において $S.(\$X)$ および $S.(S.(H(CBILL)))$ として示される。これと比較すると、図5においては、アイテム $\$X$ および $S.(H(CBILL))$ は、顧客コンピュータによって1つの連結された統一体として署名される。

## 【 0 0 5 3 】

図1から図6の電子請求書処理システムに対する他の変更例としては、請求書提示コンピュータ20を完全になくことができ；この変更例は図8に示される。図8の変更例においては、顧客コンピュータ30-m内のプログラム31は、特定の完全な請求書についての要求をビラーコンピュータ10-nに送り、この要求は、図8においては要求CBILLとして示される。ビラーコンピュータ10-n内のプログラム17はこれに応答して、完全な請求書のハッシュを計算し、ハッシュにビラーコンピュータのプライベートキー「b」でデジタル方式で署

名をする。このデジタル方式で署名されたハッシュS。(H(CBILL))および要求された完全な請求書CBILLは、次に、顧客コンピュータ30-mに送られる。

【0054】

この後、顧客コンピュータ30-m内のプログラム31は、前に説明した図4のステップS20～S24を実行し、それによって、完全な請求書が視覚的に表示され、表示された請求書に対する支払を許可することができる。もしこのような支払が許可されれば、プログラム31は時刻t1\*において電子支払サブシステム50へ支払要求メッセージPRMを送り；支払サブシステム50からの応答が時刻t11\*において受取られる。この応答を発生させるため、図8の電子支払サブシステム50内の構成要素はすべて、図7に関連して前に説明したのと同じように動作する。

【0055】

他の変更例としては、各ビラーコンピュータ10-nは、まだ完全に支払われてはいないすべての請求書を自動的に識別するよう、周期的に電子支払サブシステム50と相互作用することができる。この変更例は図8に示され、図8では、ビラーコンピュータ10-n内に上述のタスクを実行するプログラム18が設けられる。

【0056】

動作においては、ビラーコンピュータ10-n内のプログラム18は、ビラーの口座において受取られたすべての支払のリストに対するメッセージをビラーの銀行内のコンピュータX(j)に送る。コンピュータX(j)内のプログラム52bはこれに応答して、データベース52bから要求されたリストを作り、リストをビラーコンピュータ10-nに送る。

【0057】

その後、ビラーコンピュータ10-n内のプログラム18は、(受取られたリストにおいて示されているように)行なわれた支払のリストと、(ビラーのCBILLデータベース13から発生された)支払われるべき支払のリストとを比較する。完全には支払われていない請求書各々について、プログラム18は、図6

のコンピュータZに対し対応する争い解決申告DRSについての要求を送る。これらの申告は、図6のステップS35a、S35b、S41aおよびS41bに示されるように、支払われていない請求書が、顧客の誤りであるのか、またはビラーの誤りであるのか、または両方の誤りであるのかを判定するのを助けるために使用される。

【0058】

争い解決申告が、顧客が特定の請求書について支払を行なったと述べている額を支払っていないことを示すときには、ビラーコンピュータ10-n内のプログラム18は顧客コンピュータ30-mへ通知を電子的に送ることができ；この通知は、顧客が誤っていることを争い解決申告が示していることを説明できる。逆に、特定の争い解決申告が、元々顧客に送られた請求書が何らかの形で変更されていたことを示すときには、ビラーコンピュータ10-nは、ビラーの誤りが見つかったことを顧客に対して認めるメッセージを電子的に送ることができる。このようなメッセージは、顧客コンピュータ30-mに直接送ることもでき、または、顧客コンピュータに提示するよう請求書提示コンピュータ20に送ることもできる。

【0059】

他の変更例としては、さまざまなコンピュータ10-n、20、30-m、X(i)、X(j)、YおよびZの間で送られるメッセージはすべて、図1から図8に関連して説明した付加的な情報を必要に応じて含み得る。こうしたメッセージは、たとえば、支払期日、請求対象期間、請求書番号および口座番号などを含み得る。このような付加的な情報の例は、図3に示す請求書概要の上部に示される。

【0060】

同様に、コンピュータ10-n、20、30-m、X(i)、X(j)、YおよびZの間で送られるすべてのメッセージは、任意のタイプの通信チャネルを通じて送られ得る。たとえば、物理的ケーブルにあるまたは無線ネットワークにある通信チャネルを通じてメッセージを送ることができる。また、コンピュータの間の各メッセージは、メッセージが送られたただ1つのコンピュータによっての



みメッセージが受取られるのを確実にするため任意の形の暗号を使用できる。同様に、図 1 から図 8 のハッシュを発生させるため、ハッシュ機能の任意の一態様（メッセージダイジェスト、暗号化テキスト和、メッセージ整合性チェックなど）を使用することができ、図 1 から図 8 のデジタル署名を発生させるため任意のプロセスが使用できる。

【 0 0 6 1 】

他の変更例としては、顧客コンピュータ 30-m は、広範な電子入力／出力装置から選択できる。このような装置の 1 つは標準的なパーソナルコンピュータであり；しかし、代替例としては、顧客コンピュータ 30-m はまた、図 1 から図 8 に関連して説明したメッセージを送り受取ることができる、公共のキオスクまたはラップトップコンピュータまたは任意の他の手持ち型通信装置であり得る。

【 0 0 6 2 】

したがって、この発明は、特定の説明した実施例または変更例のいずれか 1 つの詳細に限定されるものではなく、添付の請求の範囲によって規定されるものであることが理解されるであろう。

【 図面の簡単な説明 】

【 図 1 】 この発明の好ましい一実施例を構成する電子請求書提示および支払システムを示す。

【 図 2 A 】 完全な請求書の一例を示し、このような完全な請求書は図 1 において C B I L L として示される。

【 図 2 B 】 完全な請求書の一例を示し、このような完全な請求書は図 1 において C B I L L として示される。

【 図 3 】 図 2 A および図 2 B の完全な請求書の概要の一例を示し、このような概要は図 1 において S B I L L として示される。

【 図 4 】 図 1 の顧客コンピュータ 30-m 内のプログラム 31 によって実行されるさまざまなステップを示す。

【 図 5 】 図 1 の請求書提示および支払システムがどのように支払サブシステム 50 と相互作用するのかを示す。

【 図 6 】 図 5 の支払サブシステム 50 内の支払決算記録が請求書の支払に

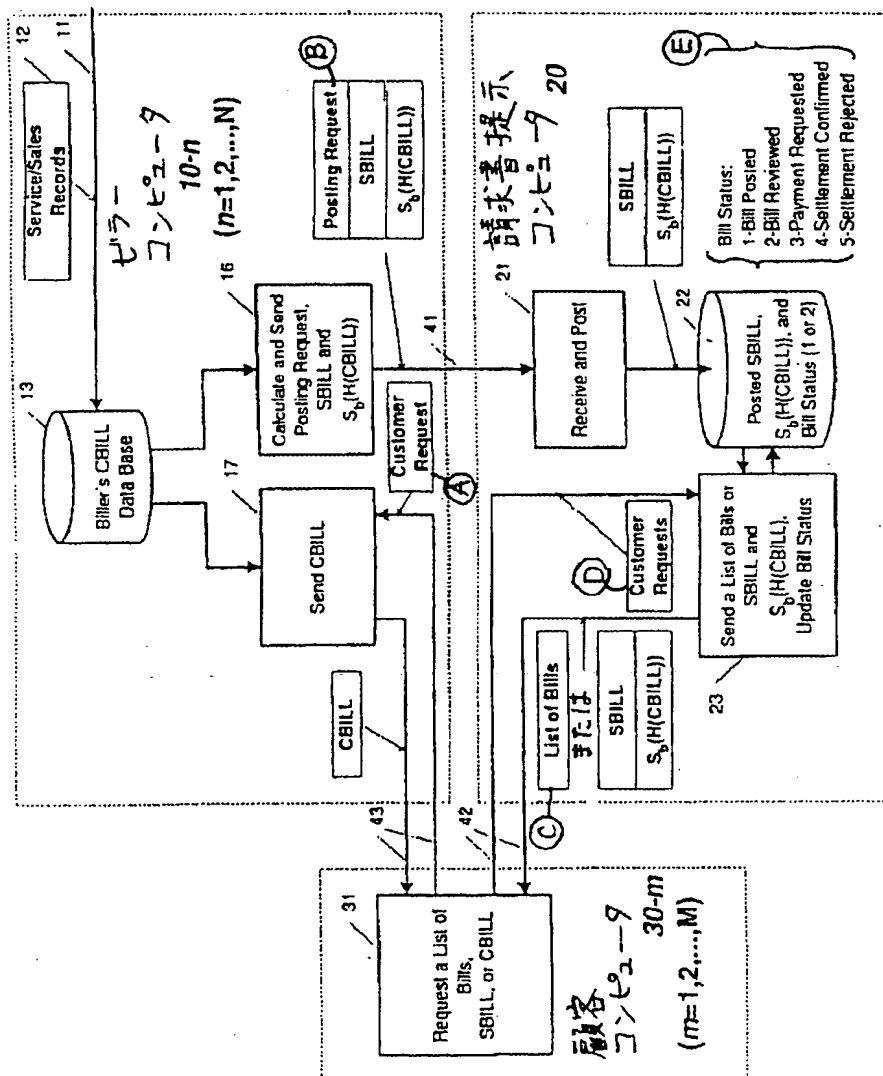
関しての争いを解決するのを助けるため、コンピュータ 2 によりどのように使用されるかを示す。

【図 7】 図 1 から図 6 の請求書提示および支払システムに対する 2 つの変更例を示す。

【図 8】 図 1 から図 6 の請求書提示および支払システムに対する 2 つの付加的な変更例を示す。

【図 1 A】

(1-1)



## 【図 1 B】

(1-2)

12の訳文：サービス／販売記録

13の訳文：ビラーのCBILLデータベース

16の訳文：ポスティング要求、SBILLおよび  
S<sub>b</sub> (H (CBILL)) を計算し送る。

17の訳文：CBILLを送る

21の訳文：受取およびポスティング

22の訳文：ポスティングされたSBILL、  
S<sub>b</sub> (H (CBILL)) および  
請求書状態 (1または2)23の訳文：請求書リストまたはSBILL  
およびS<sub>b</sub> (H (CBILL)) を送る。  
請求書状態を更新する。31の訳文：請求書リスト、SBILLまたは  
CBILLを要求する

Aの訳文：顧客の要求

Bの訳文：ポスティング要求

Cの訳文：請求書のリスト

Dの訳文：顧客の要求

Eの訳文：請求書状態：

1－ポスティングされた請求書

2－検査された請求書

3－支払要求されている

4－決済が確認されている

5－決済が拒否されている

*カリフォルニア	ベル	156	*
家屋定率サービス	提示日	ジョントー	Page 1
アカウント番号	1997年5月21日	1234 MAIN ST	
808 677-1234	227 K 0193	IRVINE, CA	92356
現在の	カリフォルニア	Page 1-7	545. 21
課金	NCI	Page 8-10	516. 68
支払期日	1997年6月11日		\$1061. 89

15A、 自宅で働く？  
あなたのホーム・オフィスを準備するお手伝いはいりませんか？ 電気通信をお使いで、電話サービスをもっとうまく利用したいとおもっていませんか？ ワーク・アット・ホーム・リソースにお電話下さい。無料でご相談にのります。tel:1-800-700-1100

日付	時刻	通話先の住所と番号	タイプ	レート	分	音信消滅料金
1.	4月21日	3:04pm LOSANGELES CA 213 874-6611	ダイヤル外	昼	1	.15
2.	4月21日	10:47pm BEVERLYHLS CA 310 648-9843	ダイヤル外	夜	2	.22
3.	4月22日	11:22am AGOURA__ CA 818 573-9984	ダイヤル外	昼	9	2.06
4.	4月22日	3:13pm LOSANGELES CA 213 874-6611	ダイヤル外	昼	7	.29
5.	4月23日	10:31pm BEVERLYHLS CA 310 648-9843	ダイヤル外	夜	2	.22
6.	4月23日	11:49am AGOURA__ CA 818 573-9984	ダイヤル外	昼	8	1.89
7.	4月24日	12:49am AGOURA__ CA 818 573-9984	ダイヤル外	昼	9	2.06
:	:	:	:	:	:	:
255.	5月20日	9:20pm LOSANGELES CA 213 778-2249	ダイヤル外	夜	7	.72
256.	5月20日	9:30pm LOSANGELES CA 213 426-1737	ダイヤル外	夜	17	1.76
257.	5月20日	9:55pm RESEDA CA 818 07-5040	ダイヤル外	夜	21	2.65
総通話料：ガルフコールド 808-677-1234						\$531.97

	説 明	額
1.	連邦通信委員会によって課金される州間通話のためのネットワーク料	7.00
2.	CAハイ・コスト・ファンドによる追加料金-A:	2.21
3.	カリフォルニア・テレネット・ファンドによる追加料金	.31
4.	ユニバーサル・テレネット・ファンドによる追加料金	2.47
5.	定率追加料金	2.37CR
6.	州規定料金	.08
7.	CA リー・サービス・アンド・コミュニケーションズ・デバイス・ファンド	.28
8.	税: 連邦税: 2.85 911: .59 地方税:	3.24
	税金と追加料金の総額	\$13.24

【 図 2 B 】

アカunt番号                      提示日                      Page 8  
 808 677-1234 235 S 0182        1997 年 5 月 21 日  
 NCI アカunt番号                  あなたの NCI 請求書についての質問は以下までどうぞ  
 7Q633529                          800-266-9963

\* N C I \* \*

長距離

808-677-1234 からの呼出

	日付	時刻	通話先の住所と番号	タイプ	レート	分	額
1.	4 月 21 日	7:25pm	SAN JOSE CA 408 244-1977	ダイヤル外	夜	1	.09
2.	4 月 21 日	7:38pm	FAIR LAWN NJ 201 705-3304	ダイヤル外	夜	1	.14
...							
83.	5 月 20 日	4:30pm	RIDLEY PARK PA 610 592-1293	ダイヤル外	昼	8	1.97
808-677-1234 からの通話料 合計							202.20
長距離料金合計							202.20

国際長距離

808-677-1234 のための NCI セイティング (商標) プラン

	日付	時刻	通話先の住所と番号	タイプ	レート	分	割引前料金
1.	4 月 21 日	9:34pm	RUSSIA 70957832217	ダイヤル外	一定	4	4.77
2.	4 月 21 日	9:40pm	Ukraine 70957832217	ダイヤル外	夜	2	2.38
...							
55.	5 月 21 日	9:44pm	RUSSIA 70958166486	ダイヤル外	夜	3	3.57
NCI セイティング プランでの 808-677-1234 からの通話料 合計							310.72
国際長距離料金合計							310.72

税金と追加料金

連邦消費税	.49
州および地方税	.02
州および地方追加料金	.04
ユニバーサル・ライフライン・テレフォン・サービス	.10
カフォルニア・リレー・サービス・アンド・コミュニケーションズ・デバイス・ファンド	.01
カフォルニア・ハイ・コスト・ファンド B 追加料金	.09
カフォルニア・テレコネクト・ファンド	.01
現在の税金および追加料金合計	.76
サービス概要	
NCI セイティング プラン (03/28/97 から 10/27/97)	3.00
長距離	202.20
国際長距離	310.72
現在の料金合計	515.92

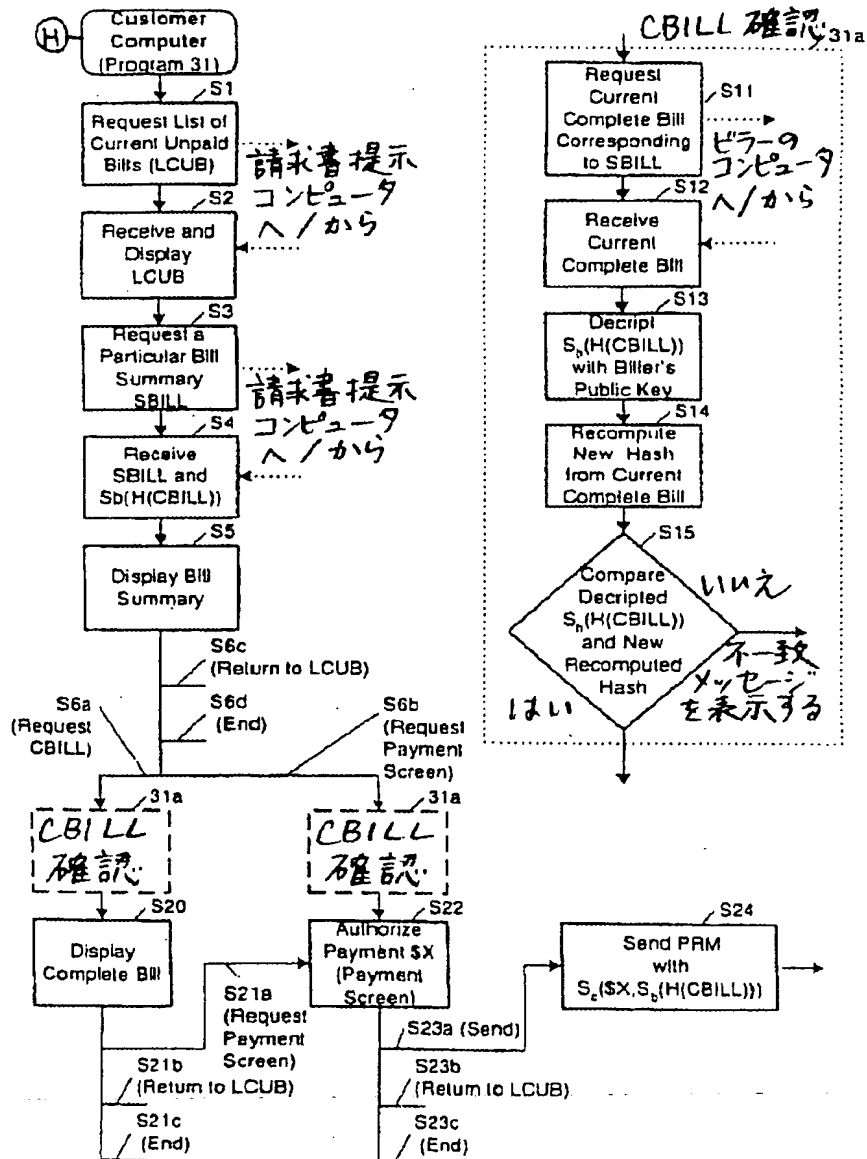
【 図 3 】

サービス/ ドラー	アカウント 番号	請求書 番号 (ID)	現在の 課金 \$	支払 期日 mm/dd/ yyyy	請求対象 期間 (開始日) mm/dd/ yyyy	請求対象 期間 (終了日) mm/dd/ yyyy	支払日を 支払った額 \$	コメント
カリフォルニア ペル	808 677- 1234 227 K 0193	1997年 5月2/日	1061.89	06/11/ 1997	04/21/ 1997	05/20/ 1997	0	

完全な請求書 を表示する	支払スクリーン を表示する	LCUBへ 戻る	終了
-----------------	------------------	-------------	----

【 図 4 A 】

( 4 - 1 )



## 【 図 4 B 】

( 4 - 2 )

H の訳文 : 顧客コンピュータ ( プログラム 3 1 )

S 1 の訳文 : 現在の未払請求書リスト ( L C U B ) を要求する

S 2 の訳文 : L C U B を受取り、表示する

S 3 の訳文 : 特定の請求書概要 ( S B I L L ) を要求する

S 4 の訳文 : S B I L L および  $S_b$  ( H ( C B I L L ) ) を受取る

S 5 の訳文 : 請求書概要を表示する

S 6 a の訳文 : ( C B I L L を要求する )

S 6 b の訳文 : ( 支払スクリーンを要求する )

S 6 c の訳文 : ( L C U B へ戻る )

S 6 d の訳文 : ( 終了 )

S 1 1 の訳文 : S B I L L に対応する現在の完全な請求書を  
要求する

S 1 2 の訳文 : 現在の完全な請求書を受取る

S 1 3 の訳文 : ビラーのパブリックキーで  
 $S_b$  ( H ( C B I L L ) ) を解説するS 1 4 の訳文 : 現在の完全な請求書から新しいハッシュを  
再び計算するS 1 5 の訳文 : 解説された  $S_b$  ( H ( C B I L L ) ) と新しく  
再び計算されたハッシュとを比較する

S 2 0 の訳文 : 完全な請求書を表示する

S 2 1 a の訳文 : ( 支払スクリーンを要求する )

S 2 1 b の訳文 : ( L C U B へ戻る )

S 2 1 c の訳文 : ( 終了 )

S 2 2 の訳文 : \$ X の支払を許可する ( 支払スクリーン )

S 2 3 a の訳文 : ( 送る )

S 2 3 b の訳文 : ( L C U B へ戻る )

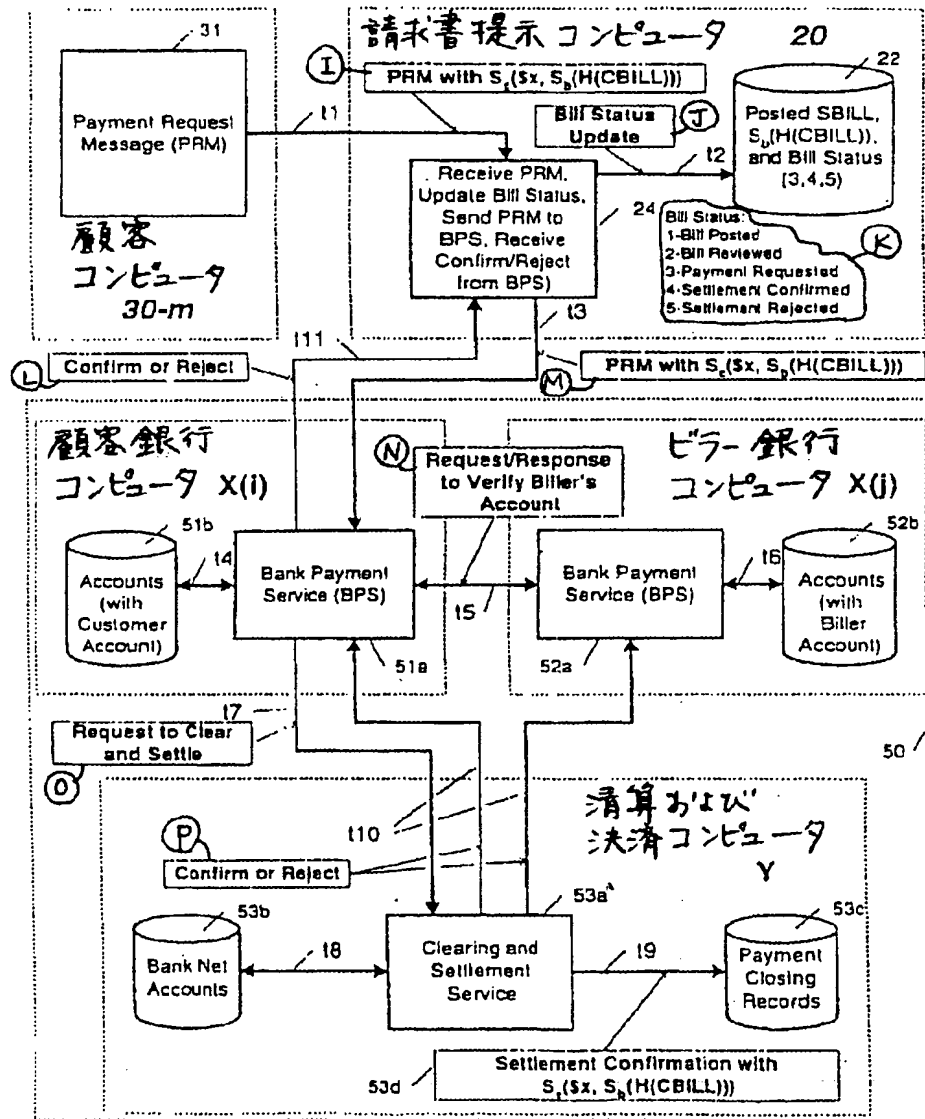
S 2 3 c の訳文 : ( 終了 )

S 2 4 の訳文 :  $S_o$  ( \$ X ,  $S_b$  ( H ( C B I L L ) ) ) を備える  
P R M を送る



【 図 5 A 】

( 5 - 1 )



## 【図5B】

(5-2)

22の訳文：ポスティングされたSBILL、

S<sub>b</sub> (H (CBILL)) および

請求書状態 (3、4、5)

24の訳文：PRMを受取り、請求書状態を更新し、

PRMをBPSへ送り、確認／拒否を

BPSから受取る

31の訳文：支払要求メッセージ (PRM)

51aの訳文：銀行支払サービス (BPS)

51bの訳文：口座 (顧客の口座を含む)

52aの訳文：銀行支払サービス (BPS)

52bの訳文：口座 (ビラーの口座を含む)

53aの訳文：清算および決済サービス

53bの訳文：銀行の純勘定

53cの訳文：支払決算記録

53dの訳文：S<sub>c</sub> (\$X, S<sub>b</sub> (H (CBILL)))

での決済確認

Iの訳文：S<sub>c</sub> (\$X, S<sub>b</sub> (H (CBILL)))

を備えるPRM

Jの訳文：請求書状態更新

Kの訳文：請求書状態：

1－ポスティングされた請求書

2－検査された請求書

3－支払要求されている

4－決済が確認されている

5－決済が拒否されている

Lの訳文：確認または拒否

Mの訳文：S<sub>c</sub> (\$X, S<sub>b</sub> (H (CBILL))) を

備えるPRM

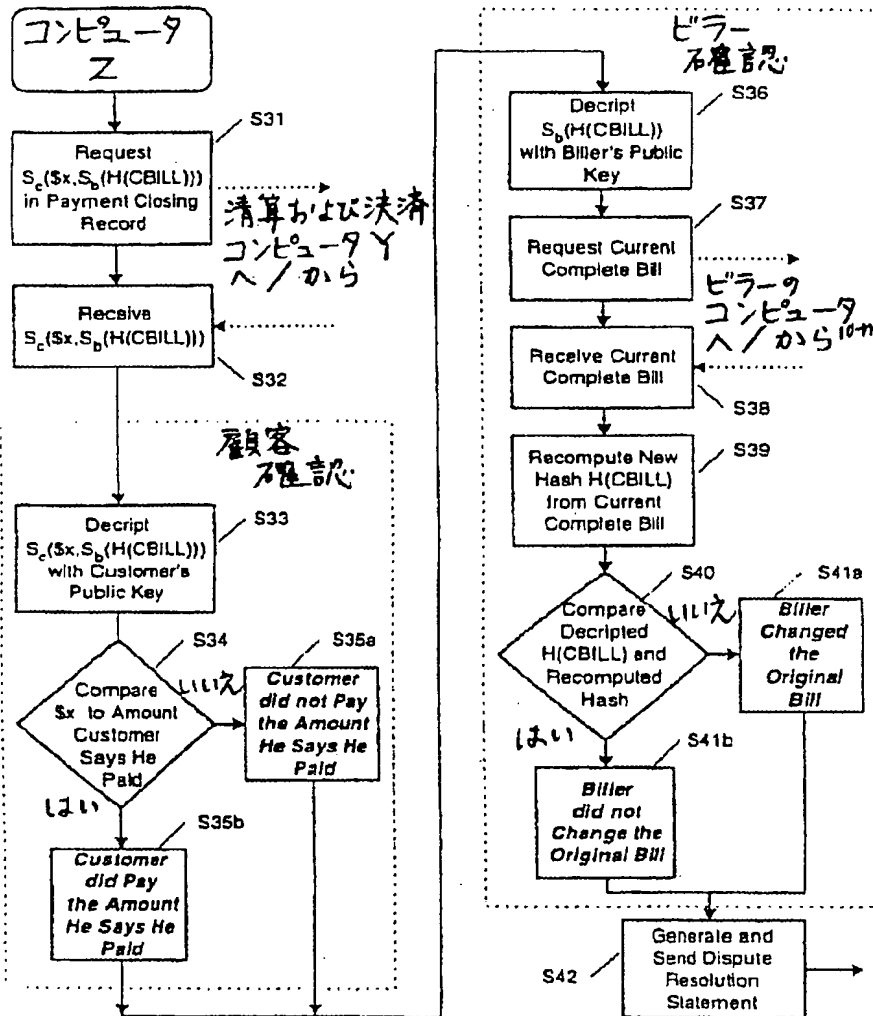
Nの訳文：ビラーの口座の確認の要求／への応答

Oの訳文：清算および決済の要求

Pの訳文：確認または拒否

【 図 6 A 】

(6-1)



## 【 図 6 B 】

( 6 - 2 )

S 3 1 の訳文 : 支払決算記録内の  $S_0$  (  $\$ X$ ,  $S_b$  (  $H$  (  $CBILL$  ) ) )

を要求する

S 3 2 の訳文 :  $S_0$  (  $\$ X$ ,  $S_b$  (  $H$  (  $CBILL$  ) ) ) を受取るS 3 3 の訳文 :  $S_0$  (  $\$ X$ ,  $S_b$  (  $H$  (  $CBILL$  ) ) ) を

顧客のパブリックキーで解読する

S 3 4 の訳文 :  $\$ X$  と顧客が支払ったと述べている額とを比較する

S 3 5 a の訳文 : 顧客は自分が払ったと述べている額を支払っていない

S 3 5 b の訳文 : 顧客は自分が払ったと述べている額を支払った

S 3 6 の訳文 :  $S_b$  (  $H$  (  $CBILL$  ) ) を銀行のパブリックキーで解読する

S 3 7 の訳文 : 現在の完全な請求書を要求する

S 3 8 の訳文 : 現在の完全な請求書を受取る

S 3 9 の訳文 : 現在の完全な請求書から新しいハッシュ  $H$  (  $CBILL$  )

を再び計算する

S 4 0 の訳文 : 解読された  $H$  (  $CBILL$  ) と再び計算された

ハッシュとを比較する

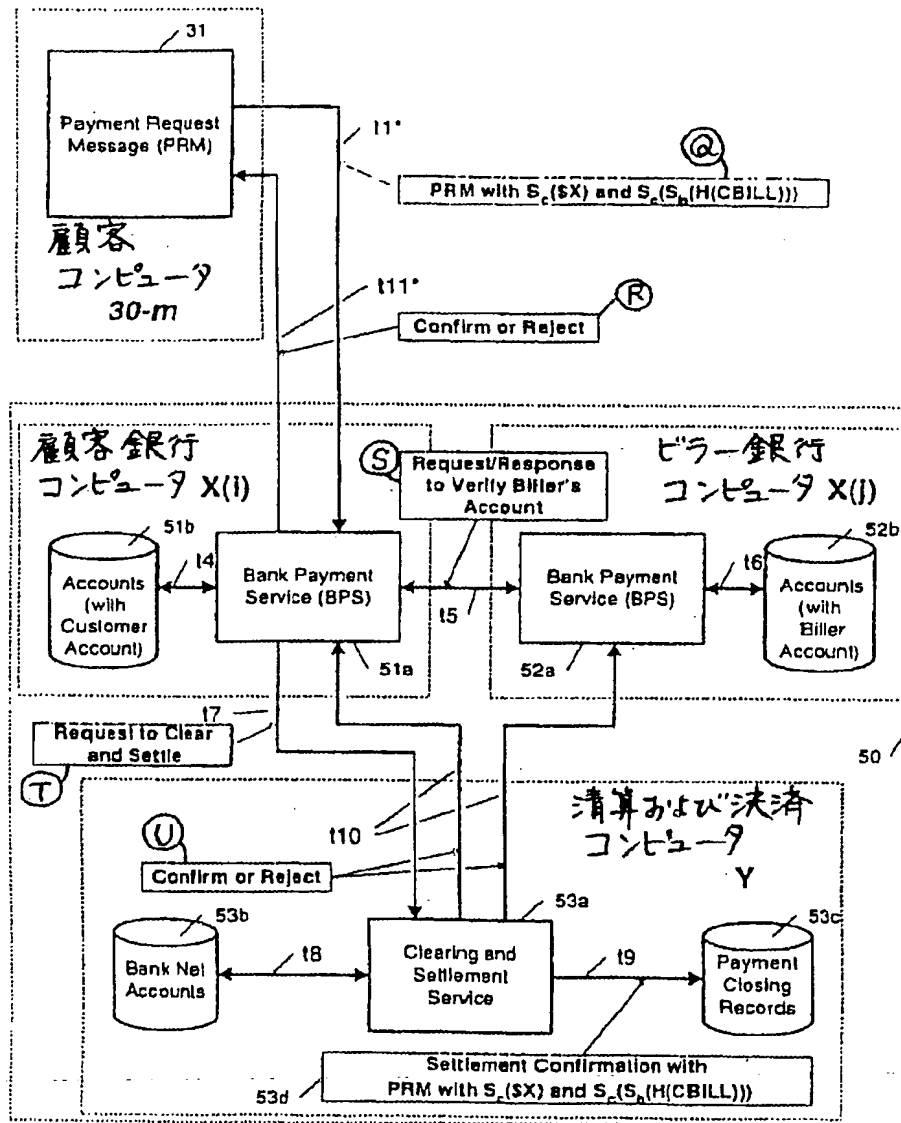
S 4 1 a の訳文 : ビラーはもとの請求書を変更した

S 4 1 b の訳文 : ビラーはもとの請求書を変更していない

S 4 2 の訳文 : 争い解決申告を発生させ、送る

【図7A】

(7-1)



## 【 図 7 B 】

( 7 - 2 )

3 1 の訳文 : 支払要求メッセージ ( P R M )

5 1 a の訳文 : 銀行支払サービス ( B P S )

5 1 b の訳文 : 口座 ( 顧客の口座を含む )

5 2 a の訳文 : 銀行支払サービス ( B P S )

5 2 b の訳文 : 口座 ( ビラーの口座を含む )

5 3 a の訳文 : 清算および決済サービス

5 3 b の訳文 : 銀行の純勘定

5 3 c の訳文 : 支払決算記録

5 3 d の訳文 :

 $S_0(\$X)$  および  $S_0(S_b(H(CBILL)))$ 

を備える P R M での決済確認

Q の訳文 :  $S_0(\$X)$  および  $S_0(S_b(H(CBILL)))$ 

を備える P R M

R の訳文 : 確認または拒否

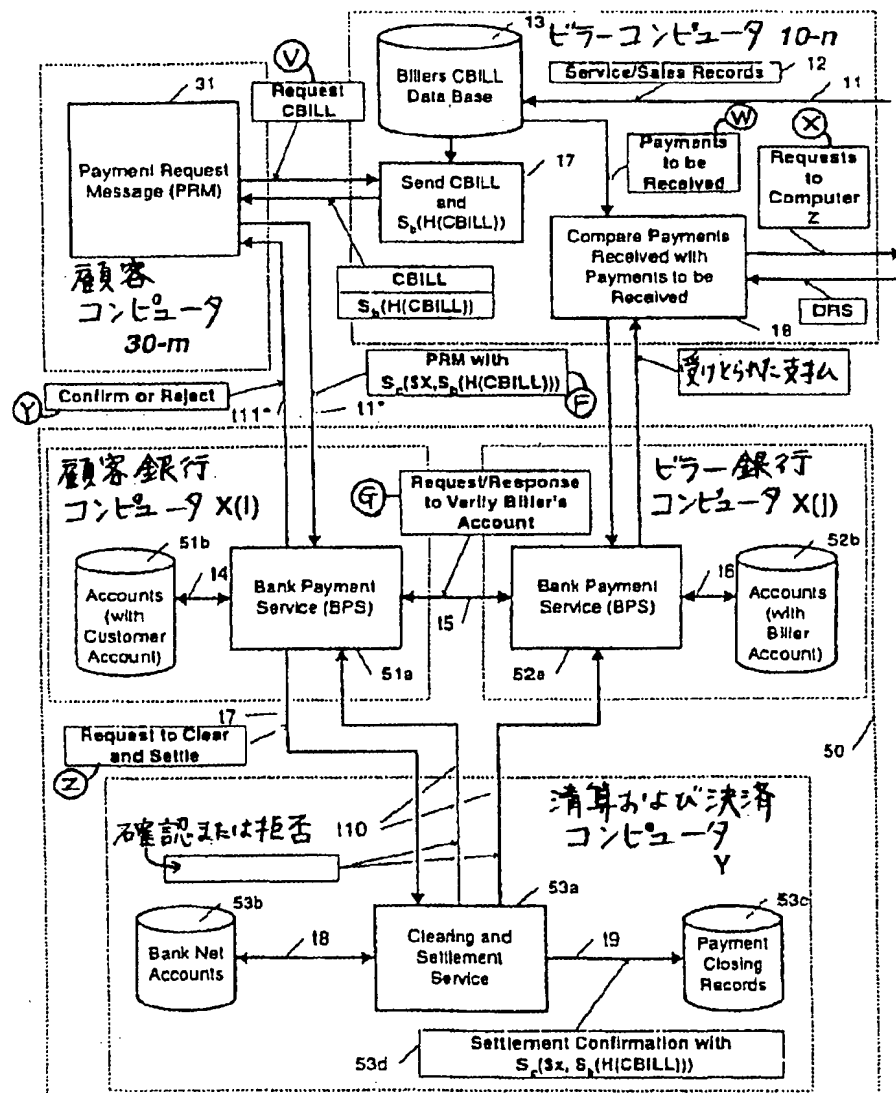
S の訳文 : ビラーの口座の確認の要求 / への応答

T の訳文 : 清算および決済の要求

U の訳文 : 確認または拒否

【 図 8 A 】

( 8 - 1 )



## 【 図 8 B 】

( 8 - 2 )

12の訳文：サービス／販売記録

13の訳文：ビラーのCBILLデータベース

17の訳文：CBILLおよび $S_b$  ( $H(CBILL)$ )  
を送る18の訳文：受取られた支払額と支払われるべき  
支払額とを比較する

31の訳文：支払要求メッセージ (PRM)

51aの訳文：銀行支払サービス (BPS)

51bの訳文：口座 (顧客の口座を含む)

52aの訳文：銀行支払サービス (BPS)

52bの訳文：口座 (ビラーの口座を含む)

53aの訳文：清算および決済サービス

53bの訳文：銀行の純勘定

53cの訳文：支払決算記録

53dの訳文： $S_c$  ( $\$X$ ,  $S_b$  ( $H(CBILL)$ ))  
を備えるPRMでの決済確認Fの訳文： $S_c$  ( $\$X$ ,  $S_b$  ( $H(CBILL)$ )) を  
備えるPRM

Gの訳文：ビラーの口座の確認の要求／への応答

Vの訳文：CBILL要求

Wの訳文：受取られるべき支払

Xの訳文：コンピュータZへの要求

Yの訳文：確認または拒否

Zの訳文：清算および決済の要求



【手続補正書】

【提出日】平成12年1月21日(2000.1.21)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 電子請求書処理システムであって、

複数の顧客のための複数の完全な請求書をストアするデータベースを有するビ  
ラーコンピュータと、

前記ビラーコンピュータに結合され、各完全な請求書の概要および前記ビラー  
コンピュータによってデジタル方式で署名された各完全な請求書のそれぞれのハ  
ッシュをストアするデータベースを有する、請求書提示コンピュータと、

前記ビラーコンピュータおよび前記請求書提示コンピュータに結合された多数  
の顧客コンピュータとを含み、特定の顧客コンピュータ各々は、a) 選択された  
完全な請求書の概要とそのそれぞれのデジタル方式で署名されたハッシュとを要  
求し前記請求書提示コンピュータから受取り、かつb) 前記選択された完全な請  
求書を要求し前記ビラーコンピュータから受取り、

前記特定の顧客コンピュータは、a) 前記選択された完全な請求書の新しいハ  
ッシュを発生させ、b) 前記選択された完全な請求書の前記デジタル方式で署名  
されたハッシュを解読し、かつc) もし解読されたデジタル方式で署名されたハ  
ッシュが前記新しく発生されたハッシュと等しくなければ、不一致が存在するこ  
とを示すことによって、前記選択された完全な請求書の受取に応答する、電子請  
求書処理システム。

【請求項2】 前記特定の顧客コンピュータはまた、前記請求書提示コンピ  
ュータに支払メッセージを送り、該支払メッセージは、a) 前記選択された完全  
な請求書の前記デジタル方式で署名されたハッシュ、およびb) 前記選択された  
完全な請求書に対する指定された額の資金の支払許可を含み、両者は前記特定の

顧客コンピュータによってデジタル方式で署名されている、請求項1に記載の電子請求書処理システム。

【請求項3】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって、1つのまとまった統一体として署名される、請求項2に記載の電子請求書処理システム。

【請求項4】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は各々、前記特定の顧客コンピュータによって別個に署名される、請求項2に記載の電子請求書処理システム。

【請求項5】 前記請求書提示コンピュータは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対しての指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによってデジタル方式で署名されているが、前記支払メッセージから獲得されたままで、前記請求書提示コンピュータのデータベースにストアすることによって、前記支払メッセージに応答する、請求項2に記載の電子請求書処理システム。

【請求項6】 前記ビラーコンピュータおよび前記顧客コンピュータと相関づけられるそれぞれの口座を保持する電子支払サブシステムをさらに含み、前記請求書提示コンピュータは、前記指定された額の資金の、前記特定の顧客コンピュータ用の口座から前記ビラー口座用の口座への移転の要求を、前記支払サブシステムへ送ることによって、前記支払メッセージに応答する、請求項2に記載の電子請求書処理システム。

【請求項7】 前記支払サブシステムは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対する指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによりデジタル方式で署名されているが、前記支払メッセージから獲得されたままで含む、決算記録をストアする、請求項6に記載の電子請求書処理システム。

【請求項 8】 前記請求書提示コンピュータはまた、a) 要求された移転が行なわれたかまたは拒否されたかを示す応答を前記支払サブシステムから受取り、かつb) 前記応答を反映するようそのデータベースを更新する、請求項 6 に記載の電子請求書処理システム。

【請求項 9】 前記請求書提示コンピュータはまた、請求書の支払が許可されたか否か、および前記支払サブシステムにおいて指定された額の資金が移転されたかまたは拒否されたかを示すメッセージを発生し前記ビラーコンピュータに送る、請求項 8 に記載の電子請求書処理システム。

【請求項 10】 前記請求書提示コンピュータはまた、前記支払サブシステムにおいて、許可された資金の移転が行なわれたかまたは拒否されたかを示すメッセージを発生し各顧客コンピュータに送る、請求項 8 に記載の電子請求書処理システム。

【請求項 11】 前記ビラーコンピュータおよび前記顧客コンピュータに相関付けされるそれぞれの口座を保持する電子支払サブシステムをさらに含み、前記特定の顧客コンピュータはまた、前記支払サブシステムに支払メッセージを送り、該支払メッセージは、a) 前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよびb) 前記選択された完全な請求書に対しての指定された額の資金の支払の許可を含み、両者は前記特定の顧客コンピュータによりデジタル方式で署名される、請求項 1 に記載の電子請求書処理システム。

【請求項 12】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって、1つのまとまった統一体として署名される、請求項 11 に記載の電子請求書処理システム。

【請求項 13】 前記支払メッセージにおいて、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記指定された額の資金の支払の前記許可は各々、前記特定の顧客コンピュータによって別個に署名される、請求項 11 に記載の電子請求書処理システム。

【請求項 14】 前記支払サブシステムは、前記選択された完全な請求書の前記デジタル方式で署名されたハッシュおよび前記選択された完全な請求書に対

する指定された額の資金の支払の前記許可を、両者とも前記特定の顧客コンピュータによりデジタル方式で署名されているが、前記支払メッセージにおいて獲得されたままで含む、決算記録をストアする、請求項11に記載の電子請求書処理システム。

【請求項15】 電子請求書処理システムであって、

複数の顧客に対し完全な請求書を発生し、ビラーコンピュータによってデジタル方式で署名された各完全な請求書のそれぞれのハッシュを発生させるビラーコンピュータと、

前記ビラーコンピュータに結合された多数の顧客コンピュータとを含み、各特定の顧客コンピュータは支払メッセージを発生し、該支払メッセージは、a) 前記ビラーコンピュータによってデジタル方式で署名された選択された完全な請求書のハッシュおよびb) 前記選択された完全な請求書に対しての指定された額の資金の支払の許可を含み、アイテムa) およびb) は両方とも前記特定の顧客コンピュータによって前記支払メッセージにおいてデジタル方式で署名され、前記システムはさらに、

前記顧客コンピュータに結合された支払サブシステムを含み、該支払サブシステムは前記支払メッセージからの、前記特定の顧客コンピュータによりデジタル方式で署名されたアイテムa) およびb) を含む決算記録をストアし、前記システムはさらに、

争い解決手段を含み、該争い解決手段は、前記ビラーコンピュータおよび前記特定の顧客コンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュを前記決算記録から読取り；前記デジタル方式で署名されたハッシュを解読して、署名されていない形の前記ハッシュを獲得し；争われている完全な請求書の新しいハッシュを発生し；前記新しいハッシュを署名されていない形の解読されたハッシュと比較する、電子請求書処理システム。

【請求項16】 争い解決手段をさらに含み、該争い解決手段は、前記特定の顧客コンピュータによってデジタル方式で署名された指定された額の資金の支払の前記許可を前記決算記録から読取り；前記デジタル方式で署名された許可を解読して、署名されていない形の前記指定された資金の額を獲得し；前記署名さ

れていない指定された資金の額と支払ったとして争われている支払の額とを比較する、請求項15に記載の電子請求書処理システム。

【請求項17】 前記支払メッセージにおいて、前記ビラーコンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって1つのまとまった統一体として署名される、請求項15に記載の電子請求書処理システム。

【請求項18】 前記支払メッセージにおいて、前記ビラーコンピュータによってデジタル方式で署名された前記選択された完全な請求書の前記ハッシュおよび前記指定された額の資金の支払の前記許可は、前記特定の顧客コンピュータによって各々別個に署名される、請求項15に記載の電子請求書処理システム。

【請求項19】 前記ビラーコンピュータおよび前記多数の顧客コンピュータに結合され、各完全な請求書の概要をストアし、前記ビラーコンピュータによりデジタル方式で署名された各完全な請求書の前記それぞれのハッシュをストアする請求書提示コンピュータをさらに含み、各顧客コンピュータは、a) 選択された完全な請求書の概要とそのそれぞれのデジタル方式で署名されたハッシュとを要求し、前記請求書提示コンピュータから受取り、b) 前記選択された完全な請求書を要求し、前記ビラーコンピュータから受取る、請求項15に記載の電子請求書処理システム。

## 【 国際調査報告 】

## INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 G06F17/60		International Application No. PCT/US 98/15190
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	WO 98 26364 A (SUN MICROSYSTEMS, INC) 18 June 1998 see abstract see page 3, last paragraph - page 5, paragraph 1 see page 6, paragraph 2 - page 8, paragraph 3 ---	16
Y	EP 0 745 947 A (IBM CORPORATION) 4 December 1996  see abstract see column 3, paragraph 2 - column 4, paragraph 1 ---	16  1-15, 17-21
A	---	
	-/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "R" document member of the same patent family		
Date of the actual completion of the international search  20 November 1998		Date of mailing of the international search report  27/11/1998
Name and mailing address of the ISA European Patent Office, P.B. 5816 Patentlaan 2 NL - 2200 HV Rijswijk Tel: (+31-70) 340-2040, Tx: 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer  Skulikaris, I

## INTERNATIONAL SEARCH REPORT

Int. Application No.

PCT/US 98/15190

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
Y	SIRBU ET AL: "NetBill: An Internet Commerce System Optimized for Network-Delivered Services" IEEE PERSONAL COMMUNICATIONS, vol. 2, no. 4, August 1995, pages 34-39, XP000517588	16
A	see page 35, left-hand column, last paragraph - page 36, right-hand column, paragraph 1 see page 37, left-hand column, paragraph 6 - page 38, left-hand column, paragraph 1	1-15, 17-21
A	US 5 649 117 A (MIDWEST PAYMENT SYSTEMS) 15 July 1997 see column 7, paragraph 2 see column 12, paragraph 3 see column 19, paragraph 4 see column 33, paragraph 3	1-21

## INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Patent Application No.

PCT/US 98/15190

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9826364 A	18-06-1998	NONE	
EP 0745947 A	04-12-1996	US 5832460 A CA 2173713 A CN 1141454 A	03-11-1998 03-12-1996 29-01-1997
US 5649117 A	15-07-1997	NONE	



---

フロントページの続き

F ターム(参考) 5B049 BB46 CC36 DD05 EE01 EE09  
FF03 FF04 FF09 GG04 GG07  
GG10  
5B055 BB20 CC10 CC13 EE02 EE21  
EE27 FA06 FB03 PA02 PA34  
PA37

【要約の続き】

て行なわれたとされる支払が許可されていたか否かについての論点を解決する際に使用するため決算記録内にストアされる。